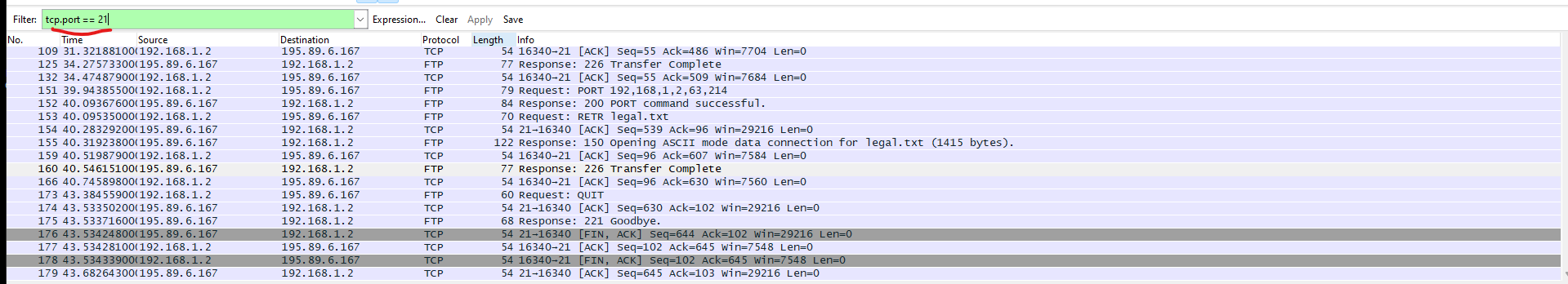
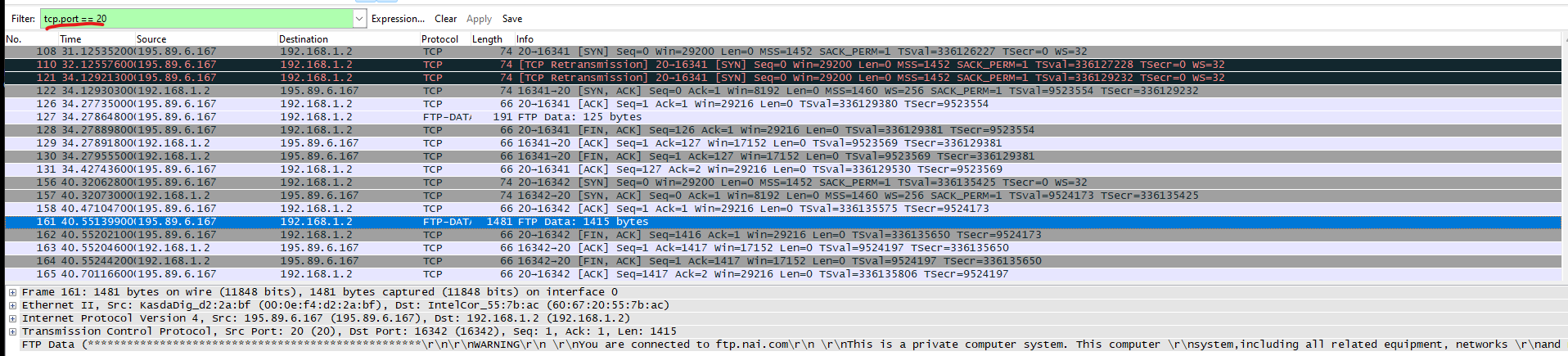
Computer Networks

Lab 4

1. FTP uses two port numbers: 20 and 21. Apply tcp.port==20 and tcp.port==21. Analyze the

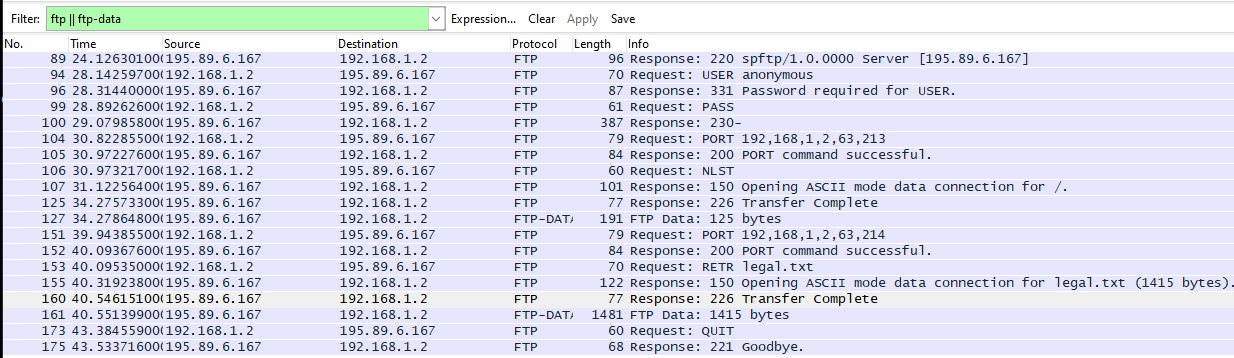
result and write down the purposes of these two ports for FTP.



Ans: Port 20 is used for transferring files during active mode FTP sessions. Port 21 is used for sending commands from the client to the server.

2. Filter out each packet using either FTP or FTP-DATA Protocol (using ftp || ftp-data filter).Mention each packet number and its purpose with reference to request made and response received in the above mentioned FTP Session in command line to get file legal.txt. Also look for Response Code and Response Arg in the FTP Header

for each packet.



1.Packet 89: Server responds to client with response code 220, which indicates that the FTP server is ready for a new client.

2.Packet 94: Client requests to server as an anonymous user.

3.Packet 96: Server responds to client saying password is required for user

4.Packet 99: Client requests server to let the user login by inputting the password.

5.Packet 100: The server sends the response code 230, which means sufficient credentials have been provided to the server to grant the user access to the FTP server.

6.Packet 104:Client asks server to send the data on IP:192.168.1.2 and Port:16341

7.Packet 105: Server sends response code 200 to client which means success, indicating it has granted the request for data successfully.

8. Packet 106: The client requests the server with NLST command which is used to retrieve a list of files from the server over a previously established data connection.

9.Packet 107: The server sends the response code 150 to the client, which means that the server has established a new connection to port 20 for data transfer. The response argument is indicates that the connection has opened in ASCII mode.

10.Packet 125: Server responds to the client with response code 226, which indicates that file transfer has completed.

11.Packet 127: Server sends data to the client.

12. Packet 151: Client requests server to send data on Port 21.

13.Packet 152: response code 200 is sent to the client from the server with the response argument PORT command successful which indicated that the server has established a connection with port 21 to send data on.

14.Packet 153: The client requests the server for the file legal.txt.

15.Packet 155: The server sends the response code 150 to the client, which means that the server has established a new connection to port 21 for data transfer.The response argument is indicates that the connection has opened in ASCII mode to send legal.txt.

16. Packet 160: Server responds to the client with response code 226, which indicates that file transfer has completed.

17. Packet 161: Server sends data(legal.txt) to the client.

18. Packet 173: Client requests to close the connection with the QUIT command to the server.

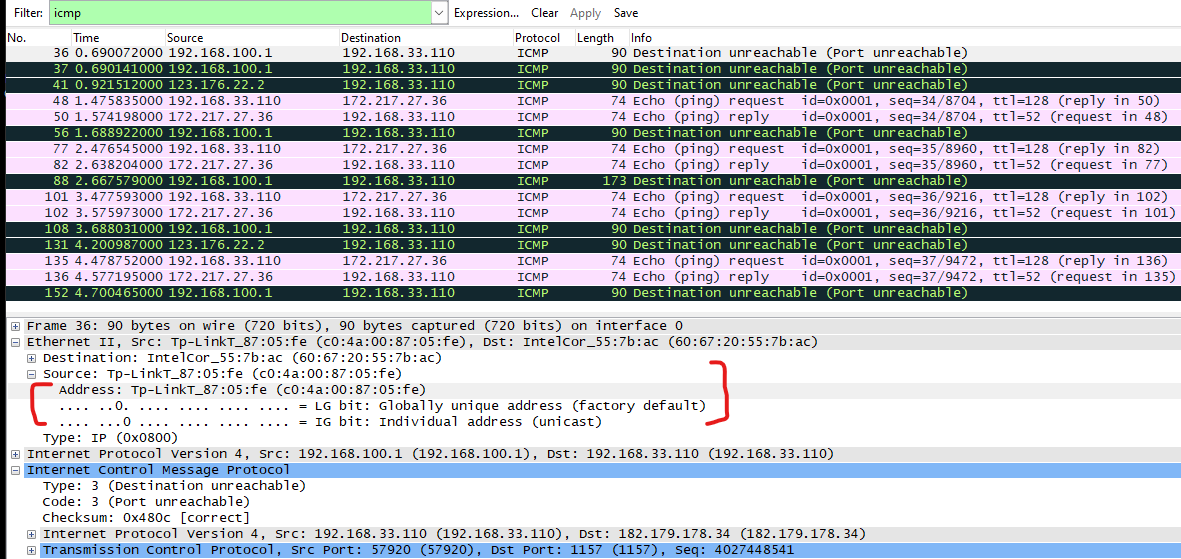
19. Packet 174: Server sends the response code 221 with the message ‘Goodbye’ to the client. It is sent immediately before the control connection is closed by the server.

Lab Statement 3: Analyzing ICMP Packets using Wireshark

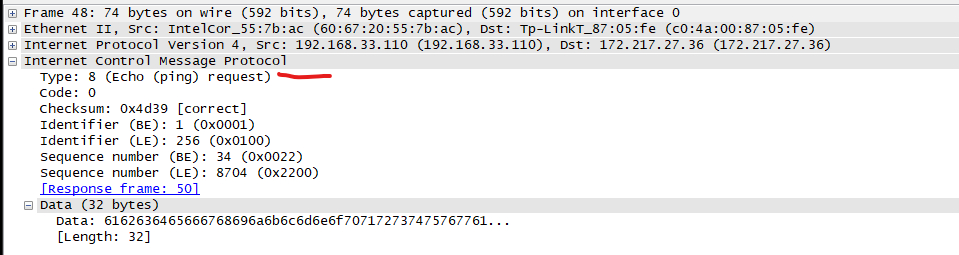
1.Are ICMP messages sent over UDP or TCP?

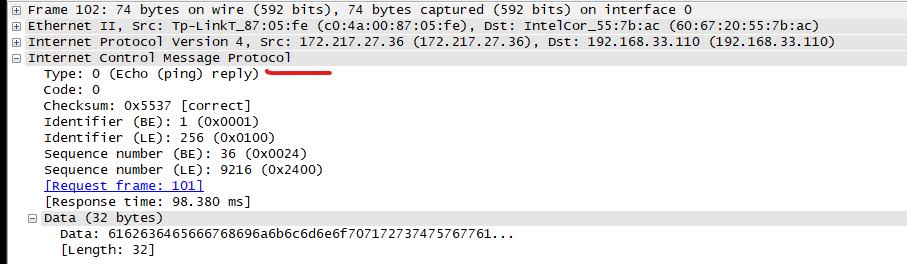
They are sent over neither, as it is a connectionless protocol. ICMP packets are transmitted in the form of datagrams with an IP header and ICMP data.

2.What is the link-layer (e.g., Ethernet) address of the host?



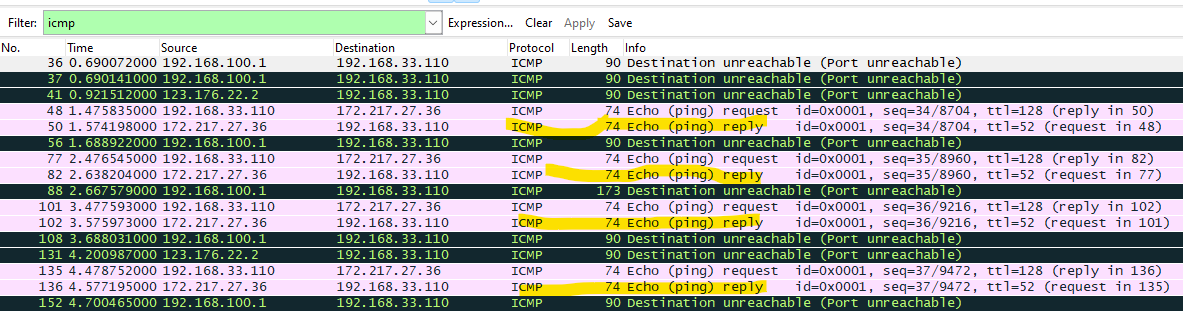
3. Which kind of request is sent through these ICMP packets?





4. How many requests are sent through the host?

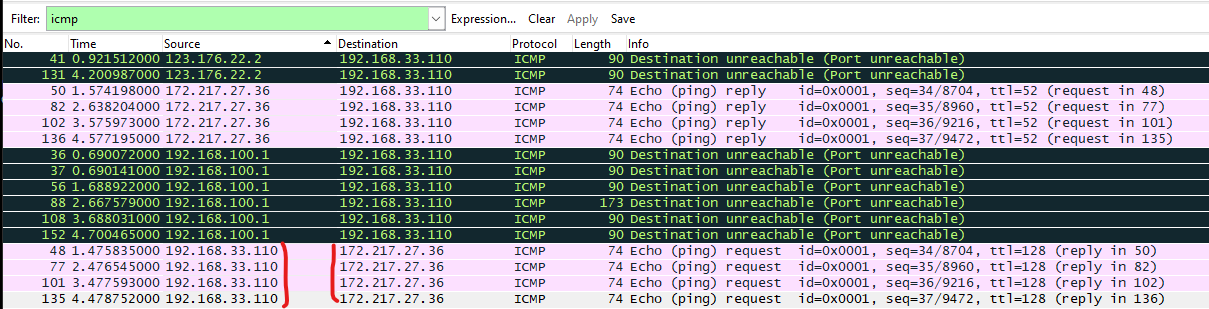
4 requests.



5. What is the IP address of your host? What is the IP address of the destination host?

IP address of host: 192.168.33.110

IP address of destination: 172.217.27.36



6. Why is it that an ICMP packet does not have source and destination port numbers?

Ans: ICMP packets do not have source and destination port numbers because they are designed to communicate network-layer information between hosts and routers, not between application-layer processes.

7. What values in the ICMP request message differentiate this message from the

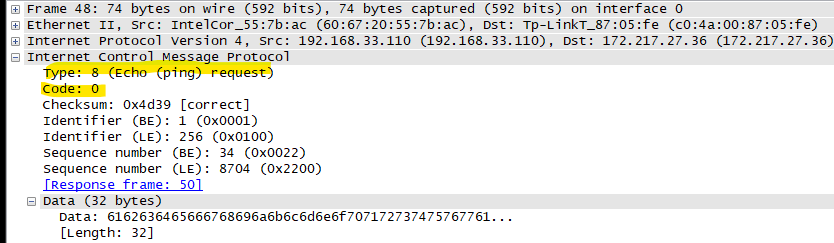
ICMP reply message?

Ans: The ICMP type differentiates whether a message is a request or a reply. The request’s type is 8 and the reply’s type is 0.

8. Examine one of the ping request packets sent by your host. What are the ICMP

type and code numbers? What other fields does this ICMP packet have? How

many bytes are the checksum, sequence number and identifier fields?



Ans:Type:8

Code:0

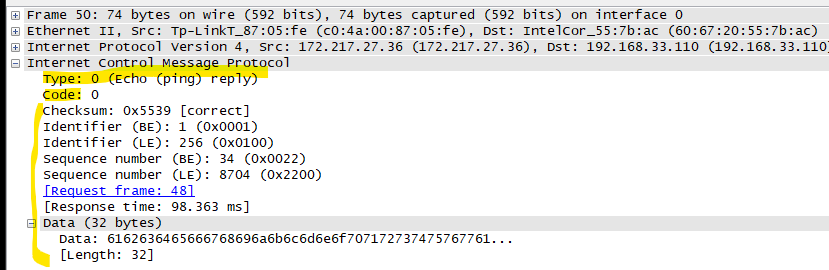
Checksum, sequence number and identifier are all 2 bytes as their length is 16bits. 16/8 = 2.

The ICMP packet has checksum, identifier, sequence number, data and its length fields.

9. Examine the corresponding ping reply packet. What are the ICMP type and code

numbers? What other fields does this ICMP packet have? How many bytes are the

checksum, sequence number and identifier fields?



Ans: Type: 0

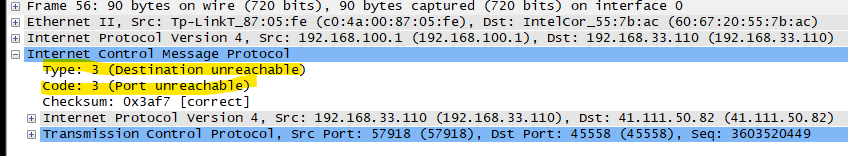
Code:0

This packet has checksum, identifier, sequence number, request frame, response time, data and its length fields.Checksum, sequence number and identifier are all 2 bytes as their length is 16bits. 16/8 = 2.

10. Examine the packet no 56. What are the ICMP type and code numbers? Why is the

IP and TCP Header included in the ICMP Header? What does these headers

Depict?



Type:3

Code:3

The type code 3 depicts that the destination is unreachable and the code shows that the destination port is unreachable.